1-2019

An attribute-based framework for secure communications in vehicular ad hoc networks

Hui CUI

Robert H. DENG
Singapore Management University, robertdeng@smu.edu.sg

Guilin WANG

Published in IEEE/ACM Transactions on Networking,
Volume 27, Issue 2, Pages 721-733, February 2019
https://doi.org/10.1109/TNET.2019.2894625

An Attribute-Based Framework for Secure Communications in Vehicular Ad Hoc Networks

Hui Cui, Robert H. Deng, *Fellow, IEEE*, and Guilin Wang

***Abstract*— In this paper, we introduce an attribute-based framework to achieve secure communications in vehicular ad hoc networks (VANETs), which enjoys several advantageous features. The proposed framework employs attribute-based signature (ABS) to achieve message authentication and integrity and protect vehicle privacy, which greatly mitigates the overhead caused by pseudonym/private key change or update in the existing solutions for VANETs based on symmetric key, asymmetric key, and identity-based cryptography and group signature. In addition, we extend a standard ABS scheme with traceability and revocation mechanisms and seamlessly integrate them into the proposed framework to support vehicle traceability and revocation by a trusted authority, and thus, the resulting scheme for vehicular communications does not suffer from the anonymity misuse issue, which has been a challenge for anonymous credential-based vehicular protocols. Finally, we implement the proposed ABS scheme using a rapid prototyping tool called Charm to evaluate its performance.**

***Index Terms*— VANET, anonymity, revocation, traceability, ABS.**

I. Introduction

VEHICULAR ad hoc networks (VANETs) are introduced to facilitate communications among vehicles and road side units (RSUs) and are envisioned to have a wide range of applications (e.g., collecting and monitoring of traffic conditions, vehicle-collision avoidance, vehicle diagnostics [1]). Obviously, communication security is crucial for the successful deployment and acceptance of VANETs.

Security in VANETs addresses issues related to authentication, integrity, protection of sensitive information such as vehicle identity and location (i.e., anonymity) and sometimes confidentiality. At the same time, authorized vehicle traceability (or non-repudiation) is important in that the identity of a vehicle can be revealed by a trusted authority (TA) if necessary such that an endorsed message's authorship can never be denied by its generator. Yet another essential and challenging problem is vehicle revocation since a vehicle's access to the vehicular network cannot be immutable and must be terminated when it is found to be compromised or caught with a misconduct.

To balance the requirements of privacy protection, authentication, integrity, non-repudiation (or traceability) and revocation, various kinds of approaches have been proposed to address the security and privacy issues in VANETs. In particular, pseudonym has been employed pervasively to achieve anonymous communications to protect vehicle privacy, and there exist a number of pseudonymity mechanisms [2] based on cryptographic primitives. Solutions using symmetric key cryptography (e.g., [3]) are computationally efficient, but they are in general not suitable for sensitive vehicle-to-vehicle communications as vehicles have to contact a base station to decrypt/verify messages received from another vehicle. Schemes based on asymmetric (or public) key cryptography (e.g., [4]) use public-key certificates without identifying information as pseudonyms, but they incur large storage and communication overheads, because public-key certificates must be sent along with messages to facilitate message verification by recipients. To remove the requirement of public-key certificates, systems on the basis of identity-based cryptography (e.g., [5]) are proposed, which exploit the implicit authentication provided by identity-based cryptography to generate unforgeable pseudonyms, but they depend on a single trusted party to issue pseudonyms. Constructions built from group signature schemes (e.g., [1]) enable a vehicle in a group to produce a signature without revealing its identity, but they assume the existence of a trusted group manager to gather vehicles into a group. Anonymous credential has also been applied for vehicular communications (e.g., [6]), but its anonymity may be misused by a malicious vehicle who could use a set of different anonymous credentials simultaneously to impersonate a number of vehicles [6]. In addition, there are protocols using attribute-based encryption (e.g., [7]–[9]) to achieve access control for vehicular communications, but they face challenges resulted from replacing pseudonyms by attributes to identify vehicles.

The pseudonyms in the approaches based on symmetric key, asymmetric key and identity-based cryptography are static in nature and need to be changed or updated frequently to avoid the linkage among different communications. Solutions built on group signature and anonymous credential schemes enable anonymous communications without asking for frequent pseudonym change or update, but when a vehicle is revoked, they either require a trusted entity (e.g., group manager) to reissue private keys to each non-revoked vehicle

Manuscript received December 5, 2016; revised August 28, 2017, February 8, 2018 and October 4, 2018; accepted January 18, 2019; approved by IEEE/ACM Transactions on Networking Editor Y. Guan. Date of publication February 5, 2019; date of current version April 16, 2019. This work was supported in part by the AXA Research Fund and in part by the National Natural Science Foundation of China under Grant 61872292. *(Corresponding author: Hui Cui.)*

H. Cui is with the School of Science, RMIT University, Melbourne, VIC 3000, Australia, and also with Data61, CSIRO, Melbourne, VIC 3000, Australia (e-mail: christi.cui.hui@gmail.com).

R. H. Deng is with the School of Information Systems, Singapore Management University, Singapore 178902.

G. Wang is with the Shield Laboratory, Central Research Institute, Huawei International Pte. Ltd., Singapore 238895.

Digital Object Identifier 10.1109/TNET.2019.2894625

(e.g., [10]) or ask to check a revocation list to discern whether the signer of a signature is revoked or not [2]. With this in mind, we ask whether it is possible to further simplify pseudonym/private key management in VANETs, and give an affirmative answer to this question in this paper.

A. Our Contributions

In this paper, we propose an attribute-based framework for secure communications in VANETs based on attribute-based signature (ABS). Since ABS enjoys a similar anonymity property as that of group signature but without requiring a group manager to collect members into a group, the proposed framework enjoys a salient advantage over existing approaches in that it avoids the need to frequently update or change vehicles' pseudonyms/private keys. In an ABS scheme, every signer is issued by the trusted authority (TA) a private attribute-key associated with a set of attributes. A valid ABS signature on a message is accompanied by a claim-predicate over a set of attributes, and attests to the fact that "a signer whose attributes satisfy the claim-predicate endorsed the message" [11]. Since the same attributes might be shared by many signers in the system, the signer's identification information is not revealed in the signature. For example, a vehicle, with a private attribute-key over attributes *City*: Sydney and *Vehicle-Type*: Bus could sign on a message associated with a claim-predicate *City*: Sydney AND *Vehicle-Type*: Bus. Any recipient of this signature can confirm that the signer is a bus from Sydney, but the vehicle's anonymity is preserved because there are many vehicles satisfying this claim-predicate.

In addition to anonymity, vehicle traceability and revocation are also critical but challenging issues, which have received equal concern in vehicular networks [2]. Unfortunately, a standard ABS scheme does not support traceability and revocation. To address these issues, we equip a standard ABS scheme with a tracing mechanism and a revocation mechanism, and seamlessly integrate them into our attribute-based framework for secure communications in VANETs. In terms of revocation, to avoid asking a revocation list to be kept to prevent revoked vehicles from sending messages or requiring the TA to issue new keys to all non-revoked vehicles (i.e., the size of key updates is linear to the number of vehicles), motivated by the revocation mechanism in [12], we incorporate a binary tree structure [13] into the key generation and key update processes in ABS, reducing the size of key updates from linear to logarithmic. Thus, in the proposed attribute-based VANET framework, the TA issues a long-term private attribute-key to each vehicle and publicly broadcasts key updates at the beginning of each time period (week, month, and so on), but only non-revoked vehicles can generate private signing keys from their long-term private attribute-keys and the key updates to sign messages over the current time period. Concerning traceability, we assign each registered vehicle a pair of public and private user-keys, and embed the public user-key in the private attribute-key generated by the TA. We subtly make the signature created using both the signing key and the private user-key by combing the signing algorithm in ABS with signature of knowledge [14] such that the TA is able to trace the vehicle when required, but no one else can learn a vehicle's identity from its signature.[1] It is worthwhile to note that due to the technique employed in the signature generation algorithm, the proposed attribute-based VANET framework simultaneously solves the traceability problem and the key escrow problem [2], where the latter implies that nobody, including the TA who issues the private attribute-key, without the private user-key of a registered vehicle, is able to create a signature on behalf of the vehicle.

In short, the contributions in this paper can be summarized as follows.

- We propose an attribute-based framework for secure communications in VANETs based on ABS, which alleviates the overhead caused by pseudonym/private key update in the existing proposals built on symmetric key, asymmetric key, identity-based cryptographic primitives and group signature schemes.
- We present a revocable and traceable ABS scheme using techniques including binary tree structure, key embedding and signature of knowledge, and seamlessly integrate them into our attribute-based framework for secure communications in VANETs to support message authentication and integrity, vehicle privacy protection, vehicle traceability and revocation by the TA.
- We implement the proposed ABS scheme using a prototyping tool called Charm [15] to evaluate its performance. The experimental results indicate that the proposed ABS scheme has the potential to be applied for secure communications in VANETs in practice.

B. Related Works

Privacy must be taken into consideration for a secure VANET [16], since a private vehicle usually carries a few passengers, with the knowledge about the position of a vehicle, one might ascertain the whereabouts of its passengers. With these goals in mind, there are schemes [3], [5], [6], [9], [10], [17]–[27] that suggest to utilize the symmetric key, public key, identity-based cryptography, group signature, anonymous credential, and attribute-based encryption, where the key challenge is to mitigate the cumbersome workload incurred by pseudonym/private key update and revocation.

The systems using the public key infrastructure (PKI) in VANETs were given in [4], [17], and [28]. Due to the use of public key certificates in this framework, they suffer from extra communication and storage overheads. The identity-based schemes for VANETs were put forth in [5], [29], and [30], which, compared to the PKI-based approach, avoid the use of certificates for public key verification and the change of public keys and the associated certificates. Unfortunately, these schemes heavily depend on the infrastructure for short-term pseudonym generation and incur high operational overhead. The constructions for VANETs based on symmetric cryptography were presented in [3], [31], and [32], which are very efficient in terms of computational and communication overheads. However, such constructions

[1] Note that due to the traceability of the TA, the anonymity is essentially the "all-or-none" anonymity.

TABLE I

COMPARISON OF PROPERTIES AMONG THE PROPOSED VANET FRAMEWORK, TAA [10] AND PUCA [27], WHERE "KEYUP" MEANS KEY UPDATES, "$\overline{\checkmark}$" DENOTES THAT IT IS NOT FULLY ACHIEVED (I.E., IT HOLDS UNDER CERTAIN CONDITIONS)

	Authentication Integrity	Anonymity	Traceability	Revocation Size of KeyUp
PUCA [27]	✓ ✓	✓	×	✓ linear
TAA [10]	✓ ✓	✓	$\overline{\checkmark}$	✓ linear
The Proposed Framework	✓ ✓	✓	✓	✓ logarithmic

are less flexible than asymmetric cryptography when it comes to vehicle authentication, since they require peer vehicles to authenticate each other via a base station. To avoid the cost associated with pseudonym update, group signature and anonymous credential based solutions were introduced in VANETs [1], [6], [10], [18], [19], [24], [26], [27]. Though group signature and anonymous credential schemes can protect privacy and ease the inconvenience caused by pseudonym change or update, they have disadvantages in that the vehicle revocation is achieved by issuing the key update for each non-revoked vehicle (i.e., the size of the key updates is linear to the number of non-revoked vehicles) or requiring a revocation list to check whether the sender of a message have been revoked. There are also protocols such as [7]–[9] built from attribute-based encryption to enable access control over secure communications in VANETs, but they have not considered potential issues (e.g., revocation, traceability) raising in VANETs when using attributes to preserve vehicle privacy. In this paper, a VANET framework based on attribute-based signature is presented to ameliorate the overheads resulted from pseudonym/private key change or update.

We compare the proposed attribute-based VANET framework with TAA [10] and PUCA [27] in Table I, which are closely relevant to our work in that both of them attempt to use digital signature schemes to achieve desirable properties required by secure communications in VANETs as ours. In TAA [10], when a vehicle is revoked, the TA communicates with each non-revoked vehicle to update their keys and thus the size of the key updates grows linearly. To trace the sender of a message, TAA [10] requires a vehicle to output another signature on this message such that it does not fully accomplishes traceability. PUCA [27] achieves vehicle revocation by storing the identification information of a revoked vehicle to a revocation list and updating the associated value of any non-revoked vehicle (via an accumulator [27]), but it does not consider tracing a malicious vehicle. In the proposed framework, the TA publicly broadcasts the key update information for all non-revoked vehicles such that the size of key updates is in a logarithmic growth. In addition, the proposed framework does not have a limitation in traceability such that it can be applied to trace any signatures generator unless the signature is not correctly created.

C. Organization

The remainder of this paper is organized as follows. In Section II, we briefly review the notions and definitions that are relevant to this paper. In Section III, after depicting the framework for secure communications in VANETs based on ABS, we present the security definitions for an ABS scheme to be used for VANETs. In Section IV, we give a detailed description of the proposed VANET framework. In Section V, we analyze the security and performance of the proposed VANET framework. Finally, we draw concluding remarks in Section VI.

II. PRELIMINARIES

In this section, we review some basic cryptographic notions and definitions that are to be used in this paper.

A. Bilinear Pairings and Complexity Assumptions

Let G be a group of a prime order p with a generator g. We define $\hat{e} : G \times G \rightarrow G_1$ to be a bilinear map if it has the following properties [33].

- Bilinear: for all $g \in G$, a, $b \in Z_p$, $\hat{e}(g^a, g^b) = \hat{e}(g, g)^{ab}$.
- Non-degenerate: $\hat{e}(g, g) \neq 1$.

We say that G is a bilinear group if the group operation in G is efficiently computable and there exists a group G_1 and an efficiently computable bilinear map $\hat{e} : G \times G \rightarrow G_1$ as above.

Diffie-Hellman Exponent Problem [34]: The l-Diffie-Hellman Exponent (l-DHE) problem is that given a tuple $(g, g^a, \ldots, g^{a^l}, g^{a^{l+2}}, \ldots, g^{a^{2l}}$ where $a \in Z_p$, it is hard to compute $(g^s, g^{a^{l+1}s})$ where $s \in Z_p$.

B. Zero-Knowledge Proof of Knowledge

In a zero-knowledge proof protocol [35], a verifier is convinced that a prover knows a certain quantity w satisfying some kind of relation R with respect to a commonly known string x, i.e., the prover convinces the verifier that he/she knows some w such that $(w, x) \in R$. If a Proof-of-Knowledge (PoK) protocol can be done in a way that the verifier learns nothing other than the validity of the statement, this protocol is called a Zero-Knowledge Proof of Knowledge (ZKPoK) protocol [35].

A PoK protocol for a binary relation R is a 3-round ZKPoK protocol between a prover P and a verifier V. For every input $(w, x) \in R$ to P and x to V, the first round of the protocol consists of P sending a commitment t to V. V then replies with a challenge c in the second round and P concludes by sending a response z in the last round. At the end of the protocol, V outputs 1 meaning "accept" or 0 otherwise. A protocol transcript (t, c, z) is *valid* if the output of an honest verifier V is accepted, called the completeness property. A PoK protocol has to satisfy the following two properties.

- Special Soundness. A cheating prover can at most answer one of many possible challenges. Specifically, there exists an efficient algorithm KE called knowledge extractor that on input x, a pair of valid transcripts (t, c, z) and (t, c', z') with $c \neq c'$, outputs w such that $(w, x) \in R$.
- Honest-Verifier Zero-Knowledge. There exists an efficient algorithm KS, called zero-knowledge simulator, that on input x and a challenge c, outputs a pair (t, z) such that

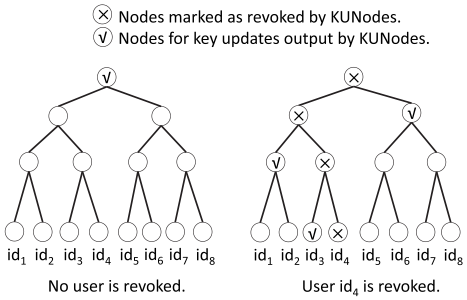


Fig. 1. Description of the KUNodes algorithm.

(t, c, z) is a valid transcript having the same distribution as a real protocol transcript resulted from the interaction between a prover P with the input $(w, x) \in R$ and an honest verifier V.

Any PoK protocol can be turned into non-interactive form, which is called Signature of Knowledge (SoK) [14], by setting the challenge to the hash value of the commitment together with the message to be signed [36].

C. Binary Tree

We follow the definition about the binary tree described in [12]. Let BT be a binary tree with N leaves corresponding to N users. Denote **root** as the root node of the tree BT. If θ is a leaf node, then Path(θ) means the set of nodes on the path from θ to **root**, including both θ and **root**. If θ is a non-leaf node, then θ_l is the left child of θ and θ_r is the right child of θ. Assume that all nodes in the tree are uniquely encoded as strings, and the tree is defined by all of its node descriptions. The KUNodes algorithm is used to compute the minimal set of nodes for which key update needs to be published so that only the non-revoked users at a time period t are able to decrypt the ciphertexts. It takes a binary tree BT, a revocation list rl and a time period t as the input, and outputs a set of nodes which is the minimal set of nodes in BT such that none of the nodes in rl with the corresponding time period before or at t (users revoked at or before t) have any ancestor (or, themselves) in the set, and all other leaf nodes (corresponding to those non-revoked users) have exactly one ancestor (or, themselves) in the set. Fig. 1 is a pictorial depiction on how the KUNodes algorithm works, where it firstly marks all ancestors of the revoked nodes as revoked, and then it outputs all non-revoked children of the revoked nodes. Below is a formal definition of the KUNodes algorithm.

KUNodes(BT, rl, t)
$X, Y \leftarrow \emptyset$.
$\forall\ (\theta_i, t_i) \in rl$, if $t_i \leq t$, then add Path(θ_i) to X.
$\forall\ x \in X$, if $x_l \notin X$, then add x_l to Y;
if $x_r \notin X$, then add x_r to Y.
If $Y = \emptyset$, then add **root** to Y.
Return Y.

D. Threshold Attribute-Based Signature

Denote $\mathbb{A}$ as the universe of possible attributes. Let $\mathbb{M}$ be the message space. In a threshold attribute-based signature (ABS) scheme [37], every message $m \in \mathbb{M}$ is signed over a claim-predicate $\Gamma_{k,S}$, where S is a subset over $\mathbb{A}$, and k is a threshold such that $1 \leq k \leq |S|$. An attribute set $\mathbf{A} \subset \mathbb{A}$ is said to satisfy $\Gamma_{k,S}$ if $|\mathbf{A} \cap S| \geq k$.

- Setup$(1^\lambda) \rightarrow (par, msk)$. On input the security parameter λ, this setup algorithm outputs the public parameter par and a master private key msk.
- KeyGen$(par, msk, \mathbf{A}) \rightarrow sk_{\mathbf{A}}$. On input the public parameter par, the master private key msk and an attribute set $\mathbf{A} \subset \mathbb{A}$ of a user, this private attribute-key generation algorithm outputs the private attribute-key $sk_{\mathbf{A}}$ for the user (assuming that the user indeed possesses these attributes).
- Sign$(par, sk_{\mathbf{A}}, \Gamma_{k,S}, m) \rightarrow \sigma$. On input the public parameter par, the signing key $sk_{\mathbf{A}}$, a claim-predicate $\Gamma_{k,S}$ where $S \subset \mathbb{A}$, $1 \leq k \leq |S|$ and a message $m \in \mathbb{M}$, this signing algorithm outputs a signature σ.
- Verify$(par, \Gamma_{k,S}, m, \sigma) \rightarrow$ *true/false*. On input the public parameter par, a claim-predicate $\Gamma_{k,S}$, a message m and a signature σ, this verification algorithm outputs *true* or *false* to denote if the signature is valid or not.

A threshold ABS scheme is correct if for any message $m \in \mathbb{M}$, any attribute set $\mathbf{A} \subset \mathbb{A}$, any claim-predicate $\Gamma_{k,S}$ $(1 \leq k \leq |S|)$ such that $|\mathbf{A} \cap S| \geq k$, $(par, msk) \leftarrow$ Setup(1^λ), $sk_{\mathbf{A}} \leftarrow$ KeyGen$(par, msk, \mathbf{A})$, $\sigma \leftarrow$ Sign$(par, sk_{\mathbf{A}}, \Gamma_{k,S}, m)$, then Verify$(par, \Gamma_{k,S}, m, \sigma) =$ *true*.

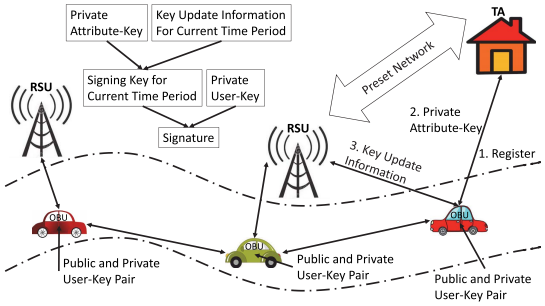


Fig. 2. A communication framework for VANETs.

III. System Architecture and Security Model

We describe the system architecture and security requirements of the attribute-based framework for secure communications in VANETs in this section.

A. System Architecture

We depict the architecture of the attribute-based VANET framework in Fig. 2, which involves a trusted authority (TA), vehicles equipped with on-board units (OBUs) for communications and road-side units (RSUs) installed alongside the roads where the OBUs and RSUs communicate over the wireless channel whereas the RSUs and the TA communicate using the fixed secure network.

In the attribute-based framework for VANETs, attribute-based signature (ABS) is employed to accomplish secure communications. Each vehicle is identified by a set of attributes (e.g., *Vehicle-Type*: Truck, *Country*: Australia, *Expiry*: 052020,

and so on) rather than a vehicle identity (VID) or a pseudonym. A regional TA publishes the public parameter and keeps the master private key for the regional VANET. When a vehicle wants to join a regional vehicular network, it must register itself to the regional TA which we call the home TA.

- Firstly, this vehicle creates a public and private user-key pair, and sends the public user-key along with other identification documents to the home TA for authentication.
- Secondly, the home TA issues this vehicle a private attribute-key over a set of attributes that it is entitled to. For example, a car who registers to the home TA serving for the city Melbourne could be given a private attribute-key over the set of attributes *City*: Melbourne, *Expiry*: 052020, *Vehicle-Type*: Car, et al.
- Thirdly, the home TA stores the public user-key of this vehicle to a list of registered vehicles such that it can trace the vehicle's identity when necessary (e.g., the vehicle may transmit a deceitful message). This traceability guarantees that a vehicle is not able to deny a message generated by itself, which simultaneously preserves non-repudiation.

The home TA periodically broadcasts the key update information at the beginning of each time period to all RSUs in its vehicular network, and then the RSUs transmit the key update information to all vehicles in the network, from which and the private attribute-key a signing key for the current time period can be extracted. In the event that a vehicle is caught with any misconduct or found to be compromised, the home TA revokes its privilege to the VANET by stopping providing the key update information for this vehicle.

Each vehicle, in order to transmit a message (e.g., the traffic condition) in the VANET, is required to authenticate this message by creating a signature on the message under a claim-predicate over an attribute set (e.g., *City*: Sydney AND *Vehicle-Type*: Bus AND *Expiry*: 052020) using the private user-key and signing key (generated from the private attribute-key and key update information) for the current time period, and this message will be accepted by others if the signature is a valid one for the given message, time period and claim-predicate. Since the same set of attributes are shared among multiple vehicles in the VANET, its private information can be protected. Any recipient can verify an endorsed message via the signature, from which it learns nothing else but the fact that a vehicle whose attributes satisfy the claim-predicate endorses the message. Clearly, due to the fact that an adversary needs to forge a valid signature for a tampered message, message integrity can be preserved from an authenticated message.

When a vehicle travels outside the home VANET, it must be authenticated by the foreign TA to enjoy the services provided by the foreign VANET. Since it is out of the scope of this paper, we omit the details here.

B. Framework

A revocable and traceable attribute-based signature (ABS) scheme consists of the following algorithms: setup algorithm Setup, user-key generation algorithm UserKG, private attribute-key generation algorithm KeyGen, key update algorithm KeyUp, signing key generation algorithm SignKG, signing algorithm Sign, verification algorithm Verify, tracing algorithm Trace and revocation algorithm Revoke.

- Setup$(1^\lambda) \rightarrow (par,\ msk,\ rl,\ st)$. Taking a security parameter λ as the input, this algorithm outputs the public parameter par, the master private key msk, an initially empty revocation list rl and a state st.
- UserKG(par, VID) $\rightarrow (sk_{vid},\ pk_{vid})$. Taking the public parameter par and a vehicle identity VID as the input, this algorithm outputs a public and private user-key pair $(sk_{vid},\ pk_{vid})$ for the vehicle VID.
- KeyGen(par, msk, pk_{vid}, $\mathbf{A}$, st) $\rightarrow (sk_{vid,\mathbf{A}},\ st)$. Taking the public parameter par, the master private key msk, a vehicle identity VID with a public user-key pk_{vid} and a set of attributes $\mathbf{A}$, as well as a state st as the input, this algorithm outputs a private attribute-key $sk_{vid,\mathbf{A}}$ for the vehicle VID with an attribute set $\mathbf{A}$ and an updated state st. Note that the TA keeps a vehicle identity list L_v storing (VID, pk_{vid}).
- KeyUp(par, msk, t, rl, st) $\rightarrow (ku_t,\ st)$. Taking the public parameter par, the master private key msk, a time period t, a revocation list rl and a state st as the input, this algorithm outputs the key update information ku_t and an updated state st.
- SignKG(par, VID, $sk_{vid,\mathbf{A}}$, ku_t) $\rightarrow sk^t_{vid,\mathbf{A}}$. Taking the public parameter par, a vehicle identity VID with the corresponding private attribute-key $sk_{vid,\mathbf{A}}$ and the key update information ku_t as the input, this algorithm outputs a signing key $sk^t_{vid,\mathbf{A}}$ for the vehicle VID for the time period t.
- Sign(par, sk_{vid}, $sk^t_{vid,\mathbf{A}}$, t, $\Gamma_{k,S}$, m) $\rightarrow \sigma$. Taking the public parameter par, the private user-key sk_{vid} and the signing key $sk^t_{vid,\mathbf{A}}$ of a vehicle VID, a time period t, a claim-predicate $\Gamma_{k,S}$ and a message M as the input, this algorithm outputs a signature σ.
- Verify($par, t, \Gamma_{k,S}, m, \sigma$) $\rightarrow$ *true/false*. Taking the public parameter par, a signature σ on a message m for a time period t under a claim-predicate $\Gamma_{k,S}$ as the input, this algorithm outputs *true* for a valid signature or *false* otherwise.
- Trace(par, msk, $(t,\ \Gamma_{k,S},\ m,\ \sigma)$, L_v) $\rightarrow$ VID. Taking the public parameter par, the master private key msk, a signature σ on a message m for a time period t under a claim-predicate $\Gamma_{k,S}$ and the vehicle identity list L_v as the input, this algorithm outputs a vehicle identity VID.
- Revoke(VID, t, rl, st) $\rightarrow rl$. Taking a vehicle identity VID to be revoked, a time period t, a revocation list rl and a state st as the input, this algorithm outputs an updated revocation list rl.

We require that a revocable and traceable ABS scheme is correct, meaning that for all attribute sets $\mathbf{A}$ and claim-predicates $\Gamma_{k,S}$ such that $\mathbf{A}$ satisfies $\Gamma_{k,S}$ (i.e., $|\mathbf{A} \wedge S| \geq k$), if $(par,\ msk,\ rl,\ st) \leftarrow$ Setup(1^λ), $(sk_{vid},\ pk_{vid}) \leftarrow$ UserKG(par, VID), $(sk_{vid,\mathbf{A}},\ st) \leftarrow$ KeyGen(par, msk, pk_{vid}, $\mathbf{A}$, st), $(ku_t,\ st) \leftarrow$ KeyUp(par, msk, t, rl, st),

$sk^t_{vid,\mathbf{A}} \leftarrow$ SignKG(par, VID, $sk_{vid,\mathbf{A}}$, ku_t), $\sigma \leftarrow$ Sign(par, sk_{vid}, $sk^t_{vid,\mathbf{A}}$, t, $\Gamma_{k,S}$, m), then Verify(par, t, $\Gamma_{k,S}$, m, σ) $\rightarrow$ *true*, Trace(par, msk, (t, $\Gamma_{k,S}$, m, σ), L_v) $\rightarrow$ VID.

C. Security Requirements and Adversarial Model

We aim to achieve the security requirements including message authentication and integrity, vehicle anonymity, traceability and revocation in the proposed attribute-based VANET framework. Authentication ensures that a message is sent by a vehicle as claimed, rather than by anyone else. Message integrity guarantees that a message has not been tampered with after the transmission. Anonymity requires that the private information of a vehicle such as VID is anonymous to anyone else in the system except the TA who is able to reveal the identity of a vehicle when required. Traceability means that the TA can discern the generator of a message via its signature, implying that a signer cannot disavow its endorsement of a message, so called non-repudiation. Revocation is needed such that a vehicle's access to a VANET can be terminated in the case that the vehicle is compromised.

Taking these requirements into account, we define unforgeability, anonymity and traceability in the adversarial model for the underlying ABS scheme. In the adversarial model, we assume that the adversary consists of a small number of active vehicles who may be in possession of some legitimate black boxes (running the defined algorithms) [10]. The adversary may use the black boxes to broadcast any messages they choose and learn the internal states (such as the random numbers used) of the black boxes. The black boxes are assumed to always correctly perform their internal operations (e.g., generating random numbers, performing other necessary operations). The aim of an adversary would be sending messages that could be accepted by others and thereby misleading them, or making the TA tracking wrong vehicles. We assume that the adversary may input an invalid message to the black box, and the black box will generate random numbers and perform other necessary operations correctly and return a correct signature on that invalid message. The aim of the adversary would be to make announcements that would be accepted by other vehicles and thereby mislead them, or to track other vehicles. We also assume that the TA or any part of the VANET infrastructure apart from the vehicles are "honest-but-curious" such that they are passive and would eavesdrop and gather information but they will honestly execute all protocols.

- Unforgeability. Any non-registered or revoked vehicle in a regional VANET has at most a negligible probability of producing a valid signature on a message for the current time period over a claim-predicate. In addition, as long as a registered vehicle is not compromised, the TA has at most a negligible probability to generate a signature on behalf of this vehicle.
- Anonymity. Nobody else except the TA who has the master private key and the list of registered vehicles has non-negligible probability to tell which vehicle generates a given signature or link multiple signatures to the same vehicle that creates them.
- Traceability. Given a signature on a message for a time period under a claim-predicate, the TA, with the master private key and the list of registered vehicles, is able to find the vehicle who generates it with overwhelming probability.

D. Security Definitions

Below we describe the formal definitions of Unforgeability, Anonymity and Traceability for the revocable and traceable ABS scheme.

Unforgeability: Unforgeability for a revocable and traceable ABS scheme is defined by the following security game between a challenger algorithm $\mathcal{C}$ and an adversary algorithm $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$, where $\mathcal{A}_1$ is any adversarial entity without the master private key, and $\mathcal{A}_2$ is the TA having the master private key.

1) Algorithm $\mathcal{A}$ is algorithm $\mathcal{A}_1$ without the master private key.
   - Setup. Algorithm $\mathcal{C}$ generates the public parameter par and the master private key msk. Algorithm $\mathcal{C}$ gives algorithm $\mathcal{A}_1$ the public parameter par.
   - Phase 1. Algorithm $\mathcal{A}_1$ issues a sequence of queries to the following oracles.
     - User-Key oracle. Algorithm $\mathcal{A}_1$ issues a private user-key query on a vehicle identity VID. Algorithm $\mathcal{C}$ returns the private user-key sk_{vid} by running the UserKG algorithm.
       Note that after algorithm $\mathcal{C}$ runs the UserKG algorithm, it adds (VID, pk_{vid}, sk_{vid}) to a list so that the same (sk_{vid}, pk_{vid}) will be used for all queries on the vehicle identity VID.
     - Attribute-Key oracle. Algorithm $\mathcal{A}_1$ issues a private attribute-key query on a vehicle identity VID with a public user-key pk_{vid} and an attribute set $\mathbf{A}$. Algorithm $\mathcal{C}$ runs the KeyGen algorithm and returns the private attribute-key $sk_{vid,\mathbf{A}}$.
     - Key-Update oracle. Algorithm $\mathcal{A}_1$ issues a key update query on a time period t. Algorithm $\mathcal{B}$ runs the KeyUp algorithm and returns the key update information ku_t.
     - Signing-Key oracle. Algorithm $\mathcal{A}_1$ issues a signing key query on a time period t, a vehicle identity VID and an attribute set $\mathbf{A}$. Algorithm $\mathcal{C}$ runs the SignKG algorithm and returns the corresponding signing key $sk^t_{vid,\mathbf{A}}$.
     - Sign oracle. Algorithm $\mathcal{A}_1$ issues a signing query on a message m, a time period t and a vehicle identity VID with attributes satisfying a claim-predicate $\Gamma_{k,S}$. Algorithm $\mathcal{C}$ runs the Sign algorithm and returns a valid signature σ.
     - Revocation oracle. Algorithm $\mathcal{A}_1$ issues a revocation query on a vehicle identity VID and a time period t. Algorithm $\mathcal{C}$ runs the Revoke algorithm and returns an updated revocation list rl.
   - Output. Algorithm $\mathcal{A}_1$ outputs a time period t^*, a claim-predicate $\Gamma^*_{k,S}$, a message m^* and a signature σ^*. Algorithm $\mathcal{A}_1$ wins the game, if (1) the

Revocation oracle has been queried on (VID, t) on $t = t^*$ or any t occurs before t^* for any vehicle identity VID whose attributes $\mathbf{A}$ satisfy $\Gamma^*_{k,S}$, (2) the Signing-Key oracle has never been queried on (VID, t^*) for any vehicle identity VID whose attributes $\mathbf{A}$ satisfy $\Gamma^*_{k,S}$, (3) (t^*, $\Gamma^*_{k,S}$, m^*) has never been queried to the Sign oracle, (4) Verify(par, t^*, $\Gamma^*_{k,S}$, m^*, σ^*) $\rightarrow$ *true*.

2) Algorithm $\mathcal{A}$ is algorithm $\mathcal{A}_2$ who is given the master private key.
   - Setup. Algorithm $\mathcal{C}$ generates the public parameter par and the master private key msk. Also, algorithm $\mathcal{C}$ generates a public and private user-key pair (pk_{vid}, sk_{vid}) for each vehicle VID, and adds the corresponding (VID, pk_{vid}) to a vehicle identity list L_v. Algorithm $\mathcal{C}$ gives algorithm $\mathcal{A}_2$ the public parameter par, the master private key msk and the vehicle identity list L_v.
   - Phase 1. Algorithm $\mathcal{A}_2$ issues the private user-key query on a vehicle identity VID, and algorithm $\mathcal{C}$ returns the private user-key.
   - Output. Algorithm $\mathcal{A}_2$ outputs a time period t^*, a claim-predicate $\Gamma^*_{k,S}$, a message m^* and a signature σ^*. Algorithm $\mathcal{A}_2$ wins the game if Verify(par, t^*, $\Gamma^*_{k,S}$, m^*, σ^*) $\rightarrow$ *true*, and Trace(par, msk, (t^*, $\Gamma^*_{k,S}$, m^*, σ^*), L_v) $\rightarrow$ VID* with the restriction that algorithm $\mathcal{A}_2$ has never issued a private user-key query on the vehicle identity VID*.

A revocable and traceable ABS scheme $\mathcal{ABS}$ is unforgeable if the advantage function referring to the above security game

$$\mathbf{Adv}^{\text{UNF}}_{\mathcal{A},\mathcal{ABS}}(\lambda) \stackrel{\text{def}}{=} \Pr[\mathcal{A} \text{ wins}]$$

is negligible in the security parameter λ for any probabilistic polynomial-time (PPT) adversary algorithm $\mathcal{A}$.

Anonymity: Anonymity for a revocable and traceable ABS scheme is defined by the following security game between a challenger algorithm $\mathcal{C}$ and an adversary algorithm $\mathcal{A}$.

- Setup. The same as that in the Unforgeability game of algorithm $\mathcal{A}_1$.
- Phase 1. The same as that in the Unforgeability game of algorithm $\mathcal{A}_1$.
- Challenge. Algorithm $\mathcal{A}$ sends two vehicle identities VID$^*_0$ and VID$^*_1$ with attributes $\mathbf{A}^*_0$ and $\mathbf{A}^*_1$ satisfying the same claim-predicate $\Gamma^*_{k,S}$, a message m^* and a time period t^* to algorithm $\mathcal{C}$. Algorithm $\mathcal{C}$ randomly chooses a bit $b \in \{0, 1\}$, generates a signature σ^* on the message m^* for the time period t^* under the claim-predicate $\Gamma^*_{k,S}$ using the private user-key $sk_{vid^*_b}$ and the corresponding signing key $sk^{t^*}_{vid^*_b,\mathbf{A}^*_b}$, and sends σ^* to algorithm $\mathcal{A}$.
- Phase 2. The same as that in Phase 1.
- Output. Algorithm $\mathcal{A}$ outputs a guess b'. If $b' = b$, algorithm $\mathcal{A}$ wins the game.

A revocable and traceable ABS scheme $\mathcal{ABS}$ achieves anonymity if the advantage function referring to the above security game

$$\mathbf{Adv}^{\text{ANON}}_{\mathcal{A},\mathcal{ABS}}(\lambda) \stackrel{\text{def}}{=} |\Pr[b = b'] - 1/2|$$

is negligible in the security parameter λ for any PPT adversary algorithm $\mathcal{A}$.

Traceability: Traceability for a revocable and traceable ABS scheme is guaranteed by the correctness of the revocable and traceable ABS scheme. Formally, for a vehicle identity VID with an attribute set $\mathbf{A}$ satisfying a claim-predicate $\Gamma_{k,S}$, if (par, msk, rl, st) $\leftarrow$ Setup(1^λ), (sk_{vid}, pk_{vid}) $\leftarrow$ UserKG(par, VID), ($sk_{vid,\mathbf{A}}$, st) $\leftarrow$ KeyGen(par, msk, pk_{vid}, $\mathbf{A}$, st), (ku_t, st) $\leftarrow$ KeyUp(par, msk, t, rl, st), $sk^t_{vid,\mathbf{A}}$ $\leftarrow$ SignKG(par, VID, $sk_{vid,\mathbf{A}}$, ku_t), $\sigma \leftarrow$ Sign(par, sk_{vid}, $sk^t_{vid,\mathbf{A}}$, t, $\Gamma_{k,S}$, m), Verify(par, t, $\Gamma_{k,S}$, m, σ) $\rightarrow$ *true*, then

$$\text{Trace}(par, msk, (t, \Gamma_{k,S}, m, \sigma), L_v) \rightarrow \text{VID}.$$

In other words, for any honestly generated signature (i.e., the signature is created following the protocol), the identity of the signer is traceable with non-negligible probability.

IV. The Proposed Framework for VANETs

In this section, we propose a revocable and traceable attribute-based signature scheme, and explain how to apply it to achieve secure communications in a vehicle network.

Define $\Delta^\Upsilon_i(x) = \prod^{j\neq i}_{j\in\Upsilon} \frac{x-j}{i-j}$ where $i \in Z_p$, and Υ is a set of elements in Z_p as the Lagrange coefficient. A polynomial $q(x)$ over Z_p with an order $d-1$ can be evaluated by using Lagrange interpolation as $q(x) = \sum_{i\in\Upsilon} q(i)\Delta_{i,\Upsilon}(x)$ where $|\Upsilon| = d$.

A. Intuition

The proposed revocable and traceable attribute-based signature (ABS) scheme is built by equipping the threshold ABS scheme given in [37] with tracing and revocation mechanisms.[2] To achieve the revocation function, the binary tree structure [13] is combined with the key generation algorithm in the ABS scheme [37] and an additional key update algorithm, where the TA issues a long-term private attribute-key to each vehicle and publicly broadcasts key updates at the beginning of each time period, but only non-revoked vehicles can generate private signing keys for the current time period from their long-term private attribute-keys and the key updates. With respect to the traceability function, each registered vehicle is assigned a pair of public and private user-keys, while the public user-key is embedded in the private attribute-key generated by the TA, and the signature is created using both the signing key and the private user-key by combing the signing algorithm in the ABS scheme [37] with signature of knowledge [14]. Thus, the signature is still attribute-based without leaking the vehicle's identity, but the TA is able to trace the vehicle who generates the signature.

B. System Setup

The home TA setups the public parameter for a vehicle network as follows, which are to be used by all algorithms within the proposed ABS scheme.

[2]Note that the techniques introduced here can be applied to other ABS schemes (e.g., [11]) to build attribute-based frameworks for secure communications in VANETs.

- Setup. On input the security parameter λ, the TA runs as follows to generate the system public parameter. Let d be the upper limit of the threshold of claim-predicate allowed in the system, and N be the maximum number of vehicles supported in the system. Let $\mathbb{A}$ be the attribute space, Ω with $|\Omega| = d$ be a default attribute set. Assume that each attribute in $\mathbb{A} \cup \Omega$ is an element from Z_p.
  1) Let $\hat{e} : G \times G \rightarrow G_1$ be a bilinear pairing where G is a group of a prime order p with a generator g. Let rl be an empty list storing revoked vehicles and BT be a binary tree with N leaf nodes. It sets st = BT. For each node x of the binary tree BT, it randomly chooses $r_x \in Z_p$, and stores r_x to this node.
  2) The TA randomly chooses $\alpha \in Z_p$, and computes $V = \hat{e}(g, g)$, $Z = V^{\alpha}$. Then it randomly chooses a vector $\vec{v} = (v_0, \ldots, v_l) \in {Z_p}^{l+1}$ where $l = 2d+1$, and computes $h_i = g^{v_i}$ for $i \in [0, l]$. In addition, it randomly chooses $f_0, \ldots, f_{n_t}, w_0, \ldots, w_{n_m} \in G$, and defines two functions F_1 and F_2 as
  $$F_1(t) = f_0 \prod_{j=1}^{n_t} {f_j}^{t_j}, \quad F_2(m) = w_0 \prod_{i=1}^{n_m} {w_i}^{m_i},$$
  where t_j is the j-th bit of a time period t and m_i is the i-th bit of a message m.
  3) The TA keeps the master private key $msk = \alpha$, and publishes the public parameter $par = (g, G, G_1, \hat{e}, p, H, V, Z, h_0, \ldots, h_l, f_0, \ldots, f_{n_t}, w_0, \ldots, w_{n_m})$, where H is a hash function mapping elements in G_1 and Z_p to an element in Z_p.

C. Vehicle Registration and Revocation

When a vehicle VID wants to join the home VANET, it firstly generates a public and private user-key pair by itself, and then sends its public user-key to the TA for registration, thereby obtaining a private attribute-key over its eligible attributes issued by the TA.

To get round achieving revocation by requiring all recipients to keep a revocation list generated by the TA or asking the TA to communicate with every non-revoked vehicle to issue new keys to them (i.e., the key update size is linear in the number of non-revoked vehicles), the binary tree data structure is combined with the key generation and update algorithms such that the TA issues every vehicle a private attribute-key at the vehicle registration phase and publicly broadcasts the key update information (i. e., the size of the key update information is logarithmic in the number of non-revoked vehicles [12]) at the beginning of each time period, but only the non-revoked vehicles are able to create signing keys for the current time period from their private attribute-keys and the key update information for the current time period.

- UserKG. On input the public parameter par and a vehicle identity VID, the vehicle randomly chooses $\beta \leftarrow Z_p^*$ as the private user-key sk_{vid}, and computes $pk_{vid} = g^{\beta}$ as the public user-key. It sends pk_{vid} along with a zero-knowledge proof of knowledge PK$\{(\beta) : pk_{vid} = g^{\beta}\}$ to the TA for registration.
- KeyGen. On input the public parameter par, the master private key msk, a public user-key pk_{vid} and an attribute set $\mathbf{A}$ of a vehicle VID and a state st, the TA firstly adds (VID, pk_{vid}) to the vehicle list L_v. Then it chooses an undefined leaf node θ from the binary tree BT, and stores the vehicle identity VID in this node. For each node $x \in$ Path(θ), it runs as follows.
  1) It fetches r_x from the node x, and randomly chooses $a_1, \ldots, a_{d-1} \in Z_p$. It defines a polynomial $q_x(w) = \sum_{i=1}^{d-1} a_i w^i + \alpha$. Then for each attribute $w \in \mathbf{A} \cup \Omega$, it randomly chooses $r_w \in Z_p$, and computes
  $$P_{x,w} = (pk_{vid}{}^{q_x(w)} / g^{r_x}) \cdot {h_0}^{r_w}, \quad P_{x,w,0} = g^{r_w},$$
  $$P_{x,w,i} = ({h_1}^{-w^i} \cdot h_{i+1})^{r_w} \quad \forall\ i \in [i, l-1].$$
  2) It sends the private attribute-key $sk_{vid,\mathbf{A}} = \{x, \{P_{x,w}, P_{x,w,0}, \{P_{x,w,i}\}_{i\in[1,l-1]}\}_{w\in\mathbf{A}\cup\Omega}\}_{x\in\text{Path}(\theta)}$ to the vehicle VID.
- KeyUp. On input the public parameter par, the master private key msk, a time period t, a revocation list rl, and a state st, the TA, for all $x \in$ KUNodes(BT, rl, t), it fetches r_x from the node x. Then, it randomly chooses $s_x \in Z_p$, and computes
  $$Q_{x,1} = g^{r_x} \cdot F_1(t)^{s_x}, \quad Q_{x,2} = g^{s_x}.$$
  It outputs the update key $ku_t = \{x, Q_{x,1}, Q_{x,2}\}_{x\in\text{KUNodes(BT, } rl, \ t)}$.
- SignKG. Denote I as Path(θ), J as KUNodes(BT, rl, t). On input the public parameter par, a private attribute-key $sk_{vid,\mathbf{A}}$, and the update key ku_t, the vehicle VID parses $sk_{vid,\mathbf{A}}$ as $\{x, \{P_{x,w}, P_{x,w,0}, \{P_{x,w,i}\}_{i\in[1,l-1]}\}_{w\in\mathbf{A}\cup\Omega}\}_{x\in I}$, ku_t as $\{x, Q_{x,1}, Q_{x,2}\}_{x\in J}$ for some set of nodes I, J. If $I \cap J = \emptyset$, it returns $\perp$. Otherwise, for any node $x \in I \cap J$, it randomly chooses $r'_w \in Z_p$. For each attribute $w \in \mathbf{A} \cup \Omega$, it computes
  $$\begin{aligned} K_w &= P_{x,w} \cdot Q_{x,1} \cdot F_1(t)^{r'_w} \\ &= pk_{vid}{}^{q_x(w)} \cdot {h_0}^{r_w} \cdot F_1(t)^{s_x + r'_w}, \\ K_{w,0} &= P_{x,w,0} = g^{r_w}, \\ K_{w,t} &= Q_{x,2} \cdot g^{r'_w} = g^{s_x + r'_w}, \\ K_{w,i} &= P_{x,w,i} = ({h_1}^{-w^i} \cdot h_{i+1})^{r_w} \quad \forall\ i \in [1, l-1]. \end{aligned}$$
  It outputs the signing key $sk^t_{vid,\mathbf{A}} = \{K_w, K_{w,0}, \{K_{w,i}\}_{i\in[1,l]}, K_{w,t}\}_{w\in\mathbf{A}\cup\Omega}$.
- Revoke. This algorithm takes a vehicle identity VID, a time period t, a revocation list rl and a state st as the input. For all nodes x associated with the vehicle identity VID, it adds (x, t) to rl, and outputs the updated revocation list rl.

D. Message Authentication

A registered vehicle VID can anonymously authenticate a message using its private user-key and signing key for the current time period over a claim-predicate. In practice, for vehicles travelling in a vehicular network, the claim-predicate $\Gamma_{k,S}$ can be set as $k = 3$, $S = \{$*City*: *, *Vehicle-Type*: *, *Expiry*: *$\}$ (the value * of each attribute depends on the real

situation), assuming that any signature that does not satisfy such a claim-predicate are not accepted by others in the VANET.

- Sign. On input the public parameter par, the private user-key sk_{vid}, the signing key $sk^t_{vid,\mathbf{A}}$ for the time period t, a claim-predicate $\Gamma_{k,S}$ and a message m, the vehicle VID runs as follows to generate a signature $\sigma = (\sigma_0, \sigma_1, \sigma_t, \sigma_2, \text{SoK}_0)$. Note that the message and signature pair (m, σ) generated by a vehicle includes five fields: (Message Type; Payload; Timestamp; TTL; Signature) [26]. Message Type field defines the message type, of which the length $L_{messagetype}$ is about 2 bytes, and the Payload field may include information on the vehicle's position, direction, speed, traffic events, event time and so on, of which the length $L_{payload}$ is about 100 bytes [26]. The Timestamp field, of which the length $L_{timestamp}$ is about 4 bytes, specifies the signature generation time, which is used to prevent replay attacks [26]. The TTL field, of which the length L_{TTL} is about 1 byte, is to determine how long the message is allowed to remain in the VANET. The Signature field is the vehicle's signature on the first four fields.
  1) It randomly chooses a subset $S' \subset \{\mathbf{A} \cap S\}$ and a default attribute subset $\Omega' \in \Omega$ such that $|S'| = k$ and $|\Omega'| = d-k$. Then, it defines a coefficient vector $\vec{b} = (b_1, \ldots, b_l) \in {Z_p}^l$ from the polynomial
  $$\varphi(y) = \prod_{w \in S \cup \Omega'} (y - w) = \sum_{i=1}^{l} b_i y^{i-1},$$
  where b_i is set to 0 for $|S \cup \Omega'| + 2 \leq i \leq l$.
  2) Denote Υ by $S' \cup \Omega'$. It computes
  $$\begin{aligned} K'_w &= K_w \cdot \prod_{i=1}^{l-1} {K_{w,i}}^{b_{i+1}} \\ &= {pk_{vid}}^{q_x(w)} \cdot (h_0 \prod_{i=1}^{l} {h_i}^{b_i})^{r_w} \cdot F_1(t)^{s_x + r'_w} \end{aligned}$$
  for each attribute $w \in \Upsilon$, and then it computes
  $$\begin{aligned} K'_0 &= \prod_{w \in \Upsilon} {K'_w}^{\Delta^{\Upsilon}_w(0)} \\ &= {pk_{vid}}^{\alpha} \cdot (h_0 \prod_{i=1}^{l} {h_i}^{b_i})^{r} \cdot F_1(t)^{r'}, \\ K'_1 &= \prod_{w \in \Upsilon} K_{w,0}^{\Delta^{\Upsilon}_w(0)} = g^r, \\ K'_t &= \prod_{w \in \Upsilon} K_{w,t}^{\Delta^{\Upsilon}_w(0)} = g^{r'}, \end{aligned}$$
  where $r = \sum_{w \in \Upsilon} \Delta^{\Upsilon}_w(0) \cdot r_w$, $r' = \sum_{w \in \Upsilon} \Delta^{\Upsilon}_w(0) \cdot (s_x + r'_w)$.
  3) It randomly chooses s, s_0, s_1, $s_2 \in Z_p$, and computes $B = Z^{\beta} \cdot V^s$,
  $$\begin{aligned} \sigma_0 &= g^s \cdot K'_0 \cdot (h_0 \prod_{i=1}^{l} {h_i}^{b_i})^{s_0} \cdot F_1(t)^{s_1} \cdot F_2(m)^{s_2}, \\ \sigma_1 &= K'_1 \cdot g^{s_0}, \quad \sigma_t = K'_t \cdot g^{s_1}, \ \sigma_2 = g^{s_2}. \end{aligned}$$
  4) It randomly chooses u_0, $u_1 \in Z_p$, and computes the signature of knowledge $\text{SoK}_0\{(s, \beta) : Y = Z^s \wedge B = Z^{\beta} \cdot V^s\}(m) = (R_1, R_2, Y, B, c, \theta_0, \theta_1)$.
  $$\begin{aligned} R_1 = Z^{u_0}, \quad R_2 = Z^{u_1} \cdot V^{u_0}, \\ c = H(R_1||R_2||Y||B||m), \\ \theta_0 = u_0 - cs, \quad \theta_1 = u_1 - c\beta. \end{aligned}$$

Remarks: In the real world, it might need to know the driving route of a vehicle in a short time period (e.g., half an hour) to make judgments about the current traffic situations, which requires messages sent by the same vehicle in a short time period to be linkable to each other. To achieve this goal, we can modify SoK_0 as $\text{SoK}_1\{(s, \beta) : Y = Z^s \wedge B = Z^{\beta} \cdot V^s \wedge A = \hat{e}(H_0(\text{Time}), h_0)^{\beta}\}(m) = (R_1, R_2, Y, B, c_1, \theta_0, \theta_1)$, where H_0 is a collision resistant hash function mapping elements in $\{0,1\}^*$ to elements in G, Time denotes the short time period (e.g., all moments between 01:00 am to 01:29 am on 17 May, 2020 are represented by 0100012917052020),

$$\begin{aligned} R_3 &= \hat{e}(H_0(\text{Time}), h_0)^{u_1}, \\ c_1 &= H(R_1||R_2||R_3||X||Y||B||A||m). \end{aligned}$$

Because all signatures generated by the same vehicle VID in the short time period Time share the a common element A, they can be easily linked together.

E. Signature Verification and Vehicle Tracing

Each recipient can check whether a message is sent by a vehicle as claimed, and has not been tampered with after the transmission by verifying the correctness of the signature on the message. Also, if a vehicle VID generates a signature on a message which is found to be deceptive, the TA can spot the vehicle identity VID of the vehicle from a given message and signature pair.

- Verify. On input the public parameter par, and a signature σ on a message m for a time period t under a claim-predicate $\Gamma_{k,S}$, the recipient computes
  $$R'_1 = Y^c \cdot Z^{\theta_0}, \quad R'_2 = B^c \cdot Z^{\theta_1} \cdot V^{\theta_0}.$$
  If $c = H(R'_1||R'_2||Y||B||m)$, it chooses the default attribute subset Ω', and obtains the vector $\vec{b} = (b_1, \ldots, b_l)$ from the polynomial $\varphi(y)$ as defined in the Sign algorithm. Then, it checks whether
  $$\frac{\hat{e}(g, \sigma_0)}{\hat{e}(h_0 \prod_{i=1}^{l} {h_i}^{b_i}, \sigma_1) \cdot \hat{e}(F_1(t), \sigma_t) \cdot \hat{e}(F_2(m), \sigma_2)} = B.$$
  It outputs *true* if the equations holds or *false* otherwise.
- Trace. On input the public parameter par, the master private key msk, a signature σ on a message m for a time period t under a claim-predicate $\Gamma_{k,S}$ and the vehicle identity list L_v, the TA checks whether there exists a pair (VID, pk_{vid}) in the vehicle identity list L_v such that $B = \hat{e}(pk_{vid}, g^{\alpha}) \cdot Y^{1/\alpha}$. If so, it outputs the vehicle identity VID.

V. Discussion

In this section, we analyze the security as well as the performance of the proposed revocable and traceable ABS scheme.

A. Security

Theorem 1: Assuming that SoK_0 is a secure signature of knowledge, then the proposed revocable and traceable ABS scheme is secure under the l-DHE assumption.

Proof: In order to prove the security of the proposed revocable and traceable ABS scheme, we need to prove that it is unforgeable, anonymous and traceable. Below we sketch the proof by showing that if there is an adversary that breaks the unforgeability, anonymity and traceability of the proposed ABS scheme, then we can build a simulator that solves the l-DHE problem or breaks the security of SoK_0.

Unforgeability: We consider two types of adversaries, where the type 1 adversaries (algorithm $\mathcal{A}_1$ in the security game) are defined to guarantee that a non-registered or revoked vehicle cannot generate a valid signature for the current time period under any claim-predicate, and the type 2 adversaries (algorithm $\mathcal{A}_2$ in the security game) are defined to ensure that anybody including the TA, without the private user-key, is not able to create a valid signature on behalf of a registered vehicle. In the proposed scheme, the signature σ can be divided into two parts, where $(\sigma_0, \sigma_1, \sigma_t, \sigma_2)$ is generated using the signing key and can prevent the type 1 adversaries, whilst SoK_0 is generated using the private user-key via a signature of knowledge scheme [35] and can prevent the type 2 adversaries. Thus, the unforgeability of the proposed ABS can be proved in terms of $(\sigma_0, \sigma_1, \sigma_t, \sigma_2)$ and SoK_0, respectively. Since $(\sigma_0, \sigma_1, \sigma_t, \sigma_2)$ is generated in the same way as that in the revocable ABS scheme [38], the proof for unforgeability for $(\sigma_0, \sigma_1, \sigma_t, \sigma_2)$ is similar to that in [38], so we omit the details here. Below we show that SoK_0 is unforgeable by proving that SoK_0 is a secure signature of knowledge. The completeness of SoK_0 is straightforward, so it remains to prove its soundness and zero-knowledge.

Soundness: Assume that there are two transcripts with the same R, R_1, R_2 but different challenges c', c and responses θ_0', θ_1' and θ_0, θ_1. Then (s, β) can be extracted from

$$\begin{aligned} R_1 &= Y^c \cdot Z^{\theta_0} = Y^{c'} \cdot Z^{\theta_0'} \Rightarrow Y = Z^s = Z^{\frac{\theta_0' - \theta_0}{c - c'}}, \\ R_2 &= B^c \cdot Z^{\theta_1} \cdot V^{\theta_0} = B^{c'} \cdot Z^{\theta_1'} \cdot V^{\theta_0'} \\ &\Rightarrow B = Z^{\beta} \cdot V^s = Z^{\frac{\theta_1' - \theta_1}{c - c'}} \cdot V^{\frac{\theta_0' - \theta_0}{c - c'}}. \end{aligned}$$

Zero-Knowledge: The simulator randomly chooses $s \in Z_p$, θ_0, $\theta_1 \in Z_p$, $c \in Z_p$, computes $R_1 = Y^c \cdot Z^{\theta_0}$, $R_2 = B^c \cdot Z^{\theta_1} \cdot V^{\theta_0}$, and sets $c = H(R_1||R_2||Y||B||m)$ where H is a random oracle.

Anonymity: Assume that $(\sigma_0, \sigma_1, \sigma_t, \sigma_2)$ is produced using a signing key corresponding to some attribute set $\mathbf{A}$ that has $\mathbf{A} \cap S \geq k$. It is not difficult to see that σ_1, σ_t, σ_2 are independent of the choice of $\mathbf{A}$. Also, according to the definition of b_i, $1 \leq i \leq l$, these values do not depend on the choice of $\mathbf{A}$, and hence σ_0 reveals no information about $\mathbf{A}$. That is, $(\sigma_0, \sigma_1, \sigma_t, \sigma_2)$ has a uniform distribution over $G \times G \times G \times G$. On the other hand, due to zero-knowledge property of signature of knowledge, SoK_0 discloses no information about the vehicle's private user-key β. Also, Y, B are randomized and independent of the choice of β. Thus, SoK_0 does not link different signatures generated by the same vehicle VID together.

Traceability: This is straightforward from the Trace algorithm. Given a signature σ, the TA with the master private key α can always discern which vehicle generates it by checking whether there exists a tuple (VID, pk_{vid}) in the vehicle identity list L_v such that $B = \hat{e}(pk_{vid}, g^{\alpha}) \cdot Y^{\frac{1}{\alpha}}$.

TABLE II

The Storage Overhead of the Proposed Revocable and Traceable ABS Scheme

	Size of Attribute -Key	Size of Signing Key	Size of Key Updates	Size of Sign-ature
Our ABS Scheme	$O((d+\lvert\mathbf{A}\rvert)\cdot(\log N+1))$	$4(d+\lvert\mathbf{A}\rvert)$	$O(R\log N/R)$ or $O(N-R)$	11 elements $\approx$ 364 bytes

TABLE III

The Computational Overhead of the Proposed Revocable and Traceable ABS Scheme

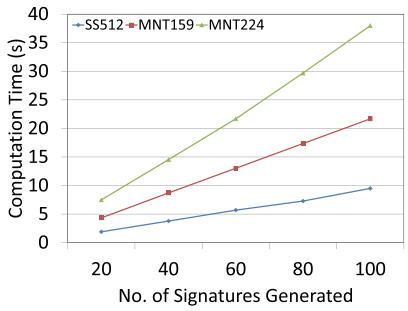
	Sign	Verify
Our ABS Scheme	$(7d+14)$E	$(2d+6)$E + 4P

B. Performance Evaluation and Implementation

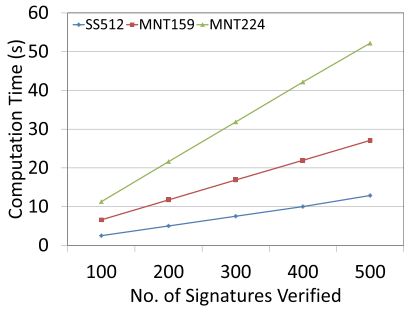
Assume that $|\mathbf{A}|$ is the number of attributes associated with a vehicle, and d is the predefined size of the default attribute set. Let "E" and "P" represent the exponentiation calculation and pairing calculation, respectively. Denote "R" and "N" as the numbers of revoked and all vehicles in the VANET, respectively. We summarize the storage overhead and the communication cost of the proposed revocable and traceable ABS scheme in Table II and Table III. The size of a private attribute-key is linear to the number of the (default) attributes possessed by a vehicle and the height of the binary tree, and a signing key is composed of $4(d + |\mathbf{A}|)$ elements from G. To sign a message, each signer performs $(7d + 14)$ exponentiation operations, while to verify the correctness of a signature, each verifier executes 4 pairing operations and $2d + 6$ exponentiation operations.[3] A signature on a message is composed of 11 elements,[4] of which 4 elements are from G, 4 elements are from G_1 and 3 elements are from Z_p. The size of key updates is logarithmic rather than linear if $1 \leq R < N/2$, and when $N/2 \leq R \leq N$, in order to keep the key update efficient, the TA will empty the revocation list and release new signing keys for the non-revoked vehicles.

[3]Note that the computational overheads resulted in the signing and verification algorithms can be reduced by applying the technology called "the server-aided computation", which has been detailed in [39] and we omit the details here.

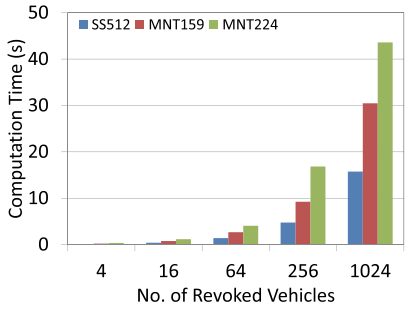
[4]To provide a security level of 112-bit, the size of the signature is about 364 bytes, while for the security level of 80-bit, the size of the signature is about 260 bytes.



(a)



(b)



(c)

Fig. 3. Computation time of the Sign (left), Verify (middle) and KeyUp (right) algorithms in the proposed revocable and traceable ABS scheme. (a) Sign. (b) Verify. (c) KeyUp.

We implement the proposed revocable and traceable ABS scheme in the Charm [15], which is a framework developed to facilitate rapid prototyping of cryptographic schemes and protocols. Since all Charm routines are designed under the asymmetric groups, the given construction is transformed to the asymmetric setting before the implementation. That is, three groups G, $\hat{G}$ and G_1 are used and the pairing $\hat{e}$ is a function from $G \times \hat{G}$ to G_1. Notice that it has been stated in [40] that the assumptions and the security proofs in the symmetric groups can be converted to those under the asymmetric setting in a generic way.

We use the Charm-0.43 and the Python 3.4 in our implementation. Along with the Charm-0.43, we install the PBC library for the underlying cryptographic operations. Our experiments are run on a laptop with Intel Core i5-4210U CPU @ 1.70GHz and 8.00 GB RAM running 64-bit Ubuntu 14.04 on the VMware Workstation Player (set with a 1GB RAM).

All of the simulations are conducted over three elliptic curves: SS512, MNT159 and MNT224, where SS512 is a symmetric curve with a 512-bit base field, MNT159 denotes an asymmetric curve with a 159-bit base field, and MNT224 represents an asymmetric curve with a 224-bit base field. These three curves provide security levels of 80-bit, 80-bit and 112-bit, respectively.

In our experiments, the number of vehicles is set to $N = 2^{20} = 1,048,576$, the size of the default attribute set is set to $d = 4$, and the threshold claim-predicate is set to $k = 3$, $S = \{$*City*: *, *Vehicle-Type*: *, *Expiry*: *$\}$. We first test the computation time for a signer in generating 20 to 100 signatures (See Fig. 3-(a)). Then, we test the computation time for a verifier in checking the validity of 100 to 500 signatures (See Fig. 3-(b)). Thereafter, we test the computation time of the TA in generating the key update information for non-revoked vehicles when the number of revoked vehicles ranges from 4 to 1024 (See Fig. 3-(c)). For the three curves used in the implementation, it is not difficult to see that SS512 has the best performance, while MNT224 incurs the highest computational overhead. The computation time of the Sign and Verify algorithms grows linearly to the number of signatures, and the computation time of the KeyUp algorithm is linear to R and logarithmic to N/R where R is the number of revoked vehicles. For the three curves tested in the experiments, the computation time of generating 20 to 100 signatures ranges from 2s to 36s, the computation time of verifying 100 to 500 signatures ranges from 3s to 60s, and the computation time of generating key updates in terms of 4 to 1024 revoked vehicles varies from 0.2s to 44s. In terms of the practical requirement for vehicular communications, the experimental results are not desirable. However, it should be noted that the code we use in the experiments is not tuned for the optimal performance. We believe that the performance can be significantly improved if the algorithms are run using the optimized codes on a more powerful computer.

VI. Conclusion

In this paper, we presented a secure VANET framework which meets the security requirements including privacy protection, authentication, traceability, revocation, message integrity and non-repudiation for VANETs. Unlike the existing solutions for secure communications in VANETs using asymmetric key, symmetric key and identity-based cryptography, group signature, anonymous credentials and attribute-based encryption as building blocks, the proposed framework is built upon an ABS scheme, which provides privacy preservation for vehicles while without the considerable overhead of managing pseudonyms/private keys, and supports the vehicle revocation and traceability by the trusted authority (TA). From the security analysis, the proposed framework satisfies various crucial security requirements. The performance of the framework can be significantly improved by incorporating techniques such as pre-computation, server-aided computation, code optimization and cryptographic hardware.

Appendix
Implementation of Attribute-Based Encryption

The proposed revocable and traceable ABS scheme for vehicular communications is attribute-based which enables

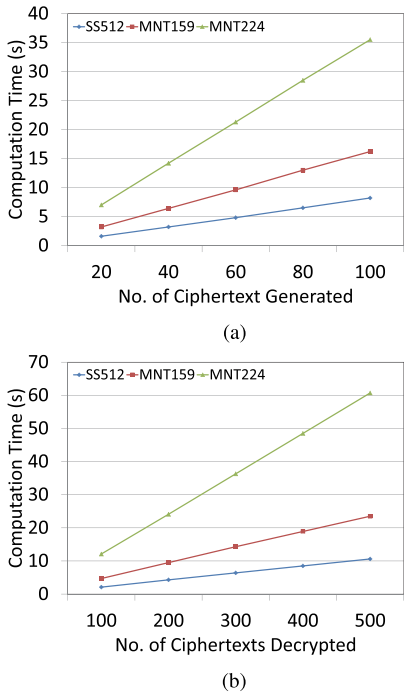


Fig. 4. Computation time of the Encrypt (left) and Decrypt (right) algorithms in an ABE scheme. (a) Encrypt. (b) Decrypt.

access control over attributes, and thus it is similar to the protocols for communications in VANETs based on attribute-based encryption (ABE). To better show the efficiency of the proposed ABS scheme, we also implement an ABE scheme which is suitable to be applied for secure communications in VANETs (e.g., [7], [8]) in Fig. 4, but it does not support the functions of vehicle revocation and traceability. Similarly, the experiments are conducted over three elliptic curves: SS512, MNT159 and MNT224. For the three curves tested in the experiments, the computation time of generating 20 to 100 ciphertexts ranges from 2s to 36s, the computation time of decrypting 100 to 500 ciphertexts ranges from 4s to 62s. It is straightforward that the proposed ABS scheme has more or less the same efficiency as the ABE based framework for vehicular communications.

Acknowledgement

The authors would like to thank the Associate Editor and the anonymous reviewers for their valuable and constructive comments.

References

[1] C.-T. Li, M.-S. Hwang, and Y.-P. Chu, "A secure and efficient communication scheme with authenticated key establishment and privacy preserving for vehicular ad hoc networks," *Comput. Commun.*, vol. 31, no. 12, pp. 2803–2814, 2008.

[2] J. Petit, F. Schaub, M. Feiri, and F. Kargl, "Pseudonym schemes in vehicular networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 1, pp. 228–255, 1st Quart., 2015.

[3] J. Y. Choi, M. Jakobsson, and S. Wetzel, "Balancing auditability and privacy in vehicular networks," in *Proc. 1st ACM Workshop Q2S Secur. Wireless Mobile Netw. (Q2SWinet)*, Montreal, QC, Canada, Oct. 2005, pp. 79–87.

[4] J. P. Hubaux, S. Capkun, and J. Luo, "The security and privacy of smart vehicles," *IEEE Secur. Privacy*, vol. 2, no. 3, pp. 49–55, May/Jun. 2004.

[5] P. Kamat, A. Baliga, and W. Trappe, "An identity-based security framework for VANETs," in *Proc. ACM 3rd Int. Workshop Veh. Ad Hoc Netw. (VANET)*, Los Angeles, CA, USA, Sep. 2007, pp. 94–95.

[6] A. Singh and H. C. S. Fhom, "Restricted usage of anonymous credentials in vehicular ad hoc networks for misbehavior detection," *Int. J. Inf. Secur.*, vol. 16, no. 2, pp. 195–211, 2017.

[7] D. Huang and M. Verma, "ASPE: Attribute-based secure policy enforcement in vehicular ad hoc networks," *Ad Hoc Netw.*, vol. 7, no. 8, pp. 1526–1535, Nov. 2009.

[8] Y. S. Rao and R. Dutta, "Efficient attribute based access control mechanism for vehicular ad hoc network," in *Proc. 7th Int. Conf. Netw. Syst. Secur. (NSS)*, in Lecture Notes in Computer Science, Madrid, Spain, vol. 7873. Berlin, Germany: Springer, Jun. 2013, pp. 26–39.

[9] Q. Kang, X. Liu, Y. Yao, Z. Wang, and Y. Li, "Efficient authentication and access control of message dissemination over vehicular ad hoc network," *Neurocomputing*, vol. 181, pp. 132–138, Mar. 2016.

[10] L. Chen, S.-L. Ng, and G. Wang, "Threshold anonymous announcement in VANETs," *IEEE J. Sel. Areas Commun.*, vol. 29, no. 3, pp. 605–615, Mar. 2011.

[11] H. K. Maji, M. Prabhakaran, and M. Rosulek, "Attribute-based signatures," in *Proc. Cryptogr. Track RSA Conf. Topics Cryptol. (CT-RSA)*, in Lecture Notes in Computer Science, San Francisco, CA, USA, vol. 6558. Berlin, Germany: Springer, Feb. 2011, pp. 376–392.

[12] A. Boldyreva, V. Goyal, and V. Kumar, "Identity-based encryption with efficient revocation," in *Proc. ACM Conf. Comput. Commun. Secur. (CCS)*, Alexandria, VA, USA, Oct. 2008, pp. 417–426.

[13] D. Naor, M. Naor, and J. Lotspiech, "Revocation and tracing schemes for stateless receivers," in *Proc. 21st Annu. Int. Cryptol. Conf. Adv. Cryptol. (CRYPTO)*, in Lecture Notes in Computer Science, Santa Barbara, CA, USA, vol. 2139. Berlin, Germany: Springer, Aug. 2001, pp. 41–62.

[14] J. Camenisch and M. Stadler, "Efficient group signature schemes for large groups," in *Advances in Cryptology—CRYPTO* (Lecture Notes in Computer Science), vol. 1294. Berlin, Germany: Springer, 1997, pp. 410–424.

[15] J. A. Akinyele *et al.*, "Charm: A framework for rapidly prototyping cryptosystems," *J. Cryptograph. Eng.*, vol. 3, no. 2, pp. 111–128, 2013.

[16] B. Hoh, M. Gruteser, H. Xiong, and A. Alrabady, "Achieving guaranteed anonymity in GPS traces via uncertainty-aware path cloaking," *IEEE Trans. Mobile Comput.*, vol. 9, no. 8, pp. 1089–1107, Aug. 2010.

[17] M. Raya and J.-P. Hubaux, "Securing vehicular ad hoc networks," in *Proc. 3rd ACM Workshop Secur. Ad Hoc Sensor Netw. (SASN)*, Alexandria, VA, USA, Nov. 2005, pp. 11–21.

[18] G. Calandriello, P. Papadimitratos, J.-P. Hubaux, and A. Lioy, "Efficient and robust pseudonymous authentication in VANET," in *Proc. ACM 4th Int. Workshop Veh. Ad Hoc Netw. (VANET)*, Montreal, QC, Canada, Sep. 2007, pp. 19–28.

[19] X. Lin, X. Sun, P.-H. Ho, and X. Shen, "GSIS: A secure and privacy-preserving protocol for vehicular communications," *IEEE Trans. Veh. Technol.*, vol. 56, no. 6, pp. 3442–3456, Nov. 2007.

[20] M. Raya, P. Papadimitratos, I. Aad, D. Jungels, and J. P. Hubaux, "Eviction of misbehaving and faulty nodes in vehicular networks," *IEEE J. Sel. Areas Commun.*, vol. 25, no. 8, pp. 1557–1568, Oct. 2007.

[21] A. Studer, E. Shi, F. Bai, and A. Perrig, "TACKing together efficient authentication, revocation, and privacy in VANETs," in *Proc. 6th Annu. IEEE Commun. Soc. Conf. Sensor, Mesh Ad Hoc Commun. Netw. (SECON)*, Rome, Italy, Jun. 2009, pp. 1–9.

[22] A. Wasef and X. Shen, "MAAC: Message authentication acceleration protocol for vehicular ad hoc networks," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Honolulu, HI, USA, Nov./Dec. 2009, pp. 1–6.

[23] H. Wen, P.-H. Ho, and G. Gong, "A novel framework for message authentication in vehicular communication networks," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Honolulu, HI, USA, Nov./Dec. 2009, pp. 1–6.

[24] Q. Wu, J. Domingo-Ferrer, and Ú. González-Nicolás, "Balanced trustworthiness, safety, and privacy in vehicle-to-vehicle communications," *IEEE Trans. Veh. Technol.*, vol. 59, no. 2, pp. 559–573, Feb. 2010.

[25] L. Zhang, Q. Wu, A. Solanas, and J. Domingo-Ferrer, "A scalable robust authentication protocol for secure vehicular communications," *IEEE Trans. Veh. Technol.*, vol. 59, no. 4, pp. 1606–1617, May 2010.

[26] B. Qin, Q. Wu, J. Domingo-Ferrer, and L. Zhang, "Preserving security and privacy in large-scale VANETs," in *Proc. 13th Int. Conf. Inf. Commun. Secur. (ICICS)*, in Lecture Notes in Computer Science, Beijing, China, vol. 7043. Berlin, Germany: Springer, Nov. 2011, pp. 121–135.

[27] D. Förster, F. Kargl, and H. Löhr, "PUCA: A pseudonym scheme with user-controlled anonymity for vehicular ad-hoc networks (VANET)," in *Proc. IEEE Veh. Netw. Conf. (VNC)*, Paderborn, Germany, Dec. 2014, pp. 25–32.
[28] K. Zeng, "Pseudonymous PKI for ubiquitous computing," in *Proc. Public Key Infrastruct., 3rd Eur. PKI Workshop, Theory Pract. (EuroPKI)*, in Lecture Notes in Computer Science, Turin, Italy, vol. 4043. Berlin, Germany: Springer, Jun. 2006, pp. 207–222.
[29] K. G. Paterson and G. Price, "A comparison between traditional public key infrastructures and identity-based cryptography," *Inf. Sec. Tech. Rep.*, vol. 8, no. 3, pp. 57–72, 2003.
[30] J. Zhang and Y. Xu, "Breaking and repairing of an anonymous and traceable communication protocol for vehicular ad hoc networks," in *Proc. 12th IEEE Int. Conf. Comput. Inf. Technol. (CIT)*, Chengdu, China, Oct. 2012, pp. 88–93.
[31] Y. Xi, K. Sha, W. Shi, L. Schwiebert, and T. Zhang, "Enforcing privacy using symmetric random key-set in vehicular networks," in *Proc. Int. Symp. Auto. Decentralized Syst. (ISADS)*, Sedona, AZ, USA, Mar. 2007, pp. 344–351.
[32] C. Zhang, X. Lin, R. Lu, and P.-H. Ho, "RAISE: An efficient RSU-aided message authentication scheme in vehicular communication networks," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Beijing, China, May 2008, pp. 1451–1457.
[33] D. Boneh and M. Franklin, "Identity-based encryption from the weil pairing," in *Advances in Cryptology—CRYPTO* (Lecture Notes in Computer Science), vol. 2139. Berlin, Germany: Springer-Verlag, 2001, pp. 213–219.
[34] D. Boneh, C. Gentry, and B. Waters, "Collusion resistant broadcast encryption with short ciphertexts and private keys," in *Proc. 25th Annu. Int. Cryptol. Conf. Adv. Cryptol. (CRYPTO)*, in Lecture Notes in Computer Science, Santa Barbara, CA, USA, vol. 3621. Berlin, Germany: Springer, Aug. 2005, pp. 258–275.
[35] S. Goldwasser, S. Micali, and C. Rackoff, "The knowledge complexity of interactive proof systems," *SIAM J. Comput.*, vol. 18, no. 1, pp. 186–208, 1989.
[36] A. Fiat and A. Shamir, "How to prove yourself: Practical solutions to identification and signature problems," in *Proc. CRYPTO*, 1986, pp. 186–194.
[37] J. Herranz, F. Laguillaumie, B. Libert, and C. Ráfols, "Short attribute-based signatures for threshold predicates," in *Proc. Cryptogr. Track RSA Conf.*, in Lecture Notes in Computer Science, San Francisco, CA, USA, vol. 7178. Berlin, Germany: Springer, Feb./Mar. 2012, pp. 51–67.
[38] J. Wei, X. Huang, X. Hu, and W. Liu, "Revocable threshold attribute-based signature against signing key exposure," in *Proc. 11th Int. Conf. Inf. Secur. Pract. Exper. (ISPEC)*, in Lecture Notes in Computer Science, Beijing, China, vol. 9065. Berlin, Germany: Springer, May 2015, pp. 316–330.
[39] H. Cui, R. H. Deng, J. K. Liu, X. Yi, and Y. Li, "Server-aided attribute-based signature with revocation for resource-constrained industrial-Internet-of-Things devices," *IEEE Trans. Ind. Informat.*, vol. 14, no. 8, pp. 3724–3732, Aug. 2018.
[40] Y. Rouselakis and B. Waters, "Practical constructions and new proof methods for large universe attribute-based encryption," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur. (CCS)*, Berlin, Germany, Nov. 2013, pp. 463–474.

Hui Cui received the Ph.D. degree from the School of Computing and Information Technology, University of Wollongong, Australia. She was a Research Fellow with the Secure Mobile Centre, School of Information Systems, Singapore Management University, Singapore. She is currently a Research Fellow (funded by the Data61, CSIRO, Australia) with the School of Science, RMIT University, Australia. Her research interests include cryptography, applied cryptography, and cloud computing.

Robert H. Deng (F'16) is currently the AXA Chair Professor of cybersecurity, the Director of the Secure Mobile Centre, and the Deputy Dean for faculty and research with the School of Information Systems, Singapore Management University (SMU). His research interests are in the areas of data security and privacy, cloud security, and Internet of Things security. He received the Outstanding University Researcher Award from the National University of Singapore, the Lee Kuan Yew Fellowship for Research Excellence from SMU, and the Asia–Pacific Information Security Leadership Achievements Community Service Star from the International Information Systems Security Certification Consortium. He served as the Steering Committee Chair for the ACM Asia Conference on Computer and Communications Security. He served on many editorial boards and conference committees, including the editorial boards of the *IEEE Security & Privacy Magazine*, the IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, the IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, the *International Journal of Information Security*, and the *Journal of Computer Science and Technology*.

Guilin Wang received the Ph.D. degree in computer science from the Institute of Software, Chinese Academy of Sciences (CAS), China, in 2001. He was a Senior Lecturer with the University of Wollongong, Australia, a Lecturer with the University of Birmingham, U.K., and a Research Scientist with the Institute for Infocomm Research, Singapore. He was an Assistant Research Professor with the Institute of Software, CAS. He joined Huawei International Pte. Ltd., Singapore, in 2013, where he is currently a Principal Engineer and focuses his research on the IoT/M2M security and privacy in the background of telecommunication. He has published over 100 research papers. His research interest is mainly in the area of applied cryptography and its applications, in particular, public key algorithms, security protocols, and communication security and privacy. In addition, he served as the Program Chair for six international security conferences, a Guest Editor for a number of international journals, and a program member of over 60 international security conferences or workshops.